



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/081,863	02/20/2002	C. Andrew Neff	324628006US3	2605

25096 7590 12/02/2005

PERKINS COIE LLP
PATENT-SEA
P.O. BOX 1247
SEATTLE, WA 98111-1247

EXAMINER

TRAN, ELLEN C

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 12/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/081,863

Applicant(s)

NEFF, C. ANDREW

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 February 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) 27-36 is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 9/2002-10/2005
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: _____

DETAILED ACTION

1. This action is responsive to communication: filed on 15 February 2002, acknowledgement that this application is a continuation in part of applications:

09/534,836 filed 24 March 2000,

09/535,927 filed 24 March 2000, and

09/816,869 filed 24 March 2001. In addition this application claims the benefit of 60/270,182 filed 20 February 2001 and 60/355,857 filed 11 February 2002.

2. Claims 1-36 are currently pending in this application. Claims 1, 9, 10, 11, 12, 20, 22, 25, 27, 32, 33, 34, 35, and 36 are independent claims.

Election/Restrictions

3. Restriction to one of the following inventions is required under 35 U.S.C. 121:

I. Claims 1-26 are drawn to a method for a voter to confirm receipt of a ballot choice with two messages, classified in class 713 subclass 175.

II. Claims 27-36 are drawn to a method for delivering two encrypted ballot components with a proof indicating that the ballot is valid to a collection system, classified in class 380 subclass 28.

4. Inventions Group I, Claims 1-26 and Group II, Claims 27-36 are related as combination and subcombination. Inventions in this relationship are distinct if it can be shown that (1) the combination as claimed does not require the particulars of the subcombination as claimed for patentability, and (2) that the subcombination has utility by itself or in other combinations (MPEP § 806.05(c)). In the instant case, the combination as claimed does not require the particulars of the subcombination as claimed because the confirmation messages can involve

Art Unit: 2134

other means besides encryption and proofs to validate the ballot choice (or message) such as counting the number of ballots received or sending a copy of the cast ballot. The subcombination has separate utility such as verifying the accuracy of transmitted data, i.e. contracts, currency, etc..

5. Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification, restriction for examination purposes as indicated is proper.

6. Because these inventions are distinct for the reasons given above and the search required for Group I is not required for Groups II, the search for Group II is not required for Group I restriction for examination purposes as indicated is proper.

7. On 17 November, 2005, examiner spoke with attorney of record Steven Lawrenz at (206) 583-8888, who later indicated by message that the applicant elects Group I without traverse, therefore claims 1-26, are currently pending, claims 1, 9, 10, 11, 12, 20, 22, and 25, are independent claims. Applicant also indicated that they plan to file a divisional for the non-elected claims 27-36.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

9. Claims 25 and 26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claim is directed to a structure and sequence for data signals, however no equipment or apparatus to form the data signal is claimed.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

11. **Claims 1, 2, 5, 9-18, 20, 22, 23, 25, and 26** are rejected under 35 U.S.C. 102(e) as being anticipated by Fujioka et al. U.S. Patent No. 6,854,447 (hereinafter ‘447).

As to independent claim 1, **“A method in a computing system for confirming receipt of a ballot choice selected by a voter, comprising: receiving a first confirmation message from a first party, the content of the first confirmation message confirming the identity of a ballot choice received for the voter by a vote collection authority; and”** is taught in ‘447 col. 7, lines 32-63;

“receiving a second confirmation message from a second party that is independent of the first party, the content of the second confirmation message independently confirming the identity of the ballot choice received for the voter by the vote collection authority” is shown in ‘447 col. 8, lines 14-36.

As to dependent claim 2, **“further comprising displaying the content of the first and second confirmation messages, such that both the displayed first confirmation message”** is disclosed in ‘447 col. 7, lines 55-62;

“and the displayed second confirmation message may be compared by the voter to expected vote confirmation messages for the ballot choice selected by the voter to determine whether a ballot choice other than the ballot choice selected by the voter has been received for the voter by the vote collection authority” is taught in ‘447 col. 8, lines 59-67.

As to dependent claim 5, “wherein the combined confirmation message is obtained using a threshold secret reconstruction technique” is shown in ‘447 col. 9, lines 21-38.

As to independent claim 9, this claim is directed to a computer-readable medium of the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 10, this claim is directed to a computing system of the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 11, this claim is directed to a computer memory device of the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 12, A method in a computing system for confirming receipt of a ballot choice selected by a voter, comprising: sending to a first recipient via a first communications channel a confirmation dictionary for a first voter containing a list of ballot choice confirmation messages ordered in a first order; and” is taught in ‘447 col. 7, lines 38-44;

“sending to the first recipient via a second communications channel that is distinct from the first communications channel a confirmation dictionary guide for the first voter indicating, for each of a plurality of valid ballot choices” is shown in ‘447 col. 7, lines 45-67;

“a position in the first order containing a ballot choice confirmation message corresponding to the valid ballot choice, such that the first recipient may use the identity of the ballot choice selected by the first voter together with the confirmation dictionary guide to identify in the confirmation dictionary the ballot choice confirmation message corresponding to the ballot choice selected by the voter” is disclosed in ‘447 col. 8, lines 1-29.

As to dependent claim 13, “wherein the first recipient is the first voter” is taught in ‘447 col. 7, lines 51-55 (It is assumed that the first voter corresponds to V_i where $i=1$).

As to dependent claim 14, “further comprising randomly selecting the first order” is shown in ‘447 col. 7, lines 52-53.

As to dependent claim 15, “further comprising sending to a second recipient via the first communications channel a second confirmation dictionary for a second voter containing a list of ballot choice confirmation messages ordered in a second order the second voter being distinct from the first voter, the second recipient being distinct from the first recipient, the second order being distinct from the first order” is disclosed in ‘447 col. 7, lines 39-60 (It is assumed that the second voter would be when $i=2$).

As to dependent claim 16, “wherein the second recipient is the second voter” is taught in ‘447 col. 7, lines 39-60.

As to dependent claim 17, “wherein the list of ballot choice confirmation messages contained in the confirmation dictionary includes a ballot choice confirmation message not corresponding to any valid ballot choice” is shown in ‘447 col. 7, lines 55-63 (Note if the ballot message is not a valid ballot choice the equation would not hold).

As to dependent claim 18, “wherein the list of ballot choice confirmation messages contained in the confirmation dictionary includes a distinguished plurality of ballot choice confirmation messages, none of the distinguished plurality of ballot choice confirmation messages corresponding to any valid ballot choice” is shown in ‘447 col. 7, lines 55-63.

As to independent claim 20, this claim is directed to a computer-readable medium of the method of claim 12; therefore it is rejected along similar rationale.

As to independent claim 22, this claim is directed to a computing system of the method of claim 12; therefore it is rejected along similar rationale.

As to dependent claim 24, “wherein the second transmission system sends the confirmation dictionary guide via a postal mail message” is taught in ‘447 col. 7, lines 40-51.

As to dependent claim 25, this claim contains substantially similar subject matter as independent claim 12; therefore it is rejected along similar rationale.

As to dependent claim 26, “wherein the ballot confirmation strings that correspond to valid ballot choices is a proper subset of the ballot confirmation strings in the sequence” is shown in ‘447 col. 7, lines 56-61.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. **Claims 3, 4, 19, and 21** are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘447 in further view of Challener et al. U.S. Patent No. 6,081,793 (hereinafter ‘793).

As to dependent claim 3, the following is not taught in ‘447: **“further comprising: combining the content of the first and second confirmation messages to obtain a combined confirmation message; and displaying the combined confirmation message, such that the displayed combined confirmation message may be compared by the voter to an expected combined vote confirmation message for the ballot choice selected by the voter to determine whether a ballot choice other than the ballot choice selected by the voter has been received for the voter by the vote collection authority”** however ‘793 teaches “FIG. 9D depicts the process after the voter has completed the ballot. As is shown in FIG. 9D, the voter encrypts the completed vote with the public key of the ballot counter "CX." The voter then encrypts the encrypted completed vote with the private key of the voter. The voter then concatenates or adds the voter ID to the encrypted information and encrypts the entire package with the public key of the authenticator "AX." The entire package is sent to the authenticator. (*‘first confirmation message’*) The authenticator verifies the vote is from the voter utilizing the

public key of the voter "VX," but the authenticator cannot read the actual completed vote, thus ensuring privacy of the voting choices, since it is encrypted with the ballot counter's public key "CX." The authenticator checks to see if this vote is the first vote for this voter and if it has a valid time stamp. If so, the authenticator stores a copy of the encrypted message that came into storage (as is shown). The authenticator then wraps up what it is able to decrypt with its private key "AO" and then appends an "add" message or sign to the message which indicates that the contents of the ballot should be added to the total vote count. The authenticator then sends this information to the ballot counter (*second confirmation message*). Preferably, the authenticator also sends back a copy of this entire message (that was sent to the ballot counter) to the voter, wrapped in the voter's public key "VX" to demonstrate to the voter that his or her vote has been counted (*'displaying the combined confirmation messages'*). The voter can compare the vote sent to the ballot counter to the vote that he or she sent the authenticator, as encrypted" in col. 10, lines 6-33.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '447 an electronic voting method to include a means to verify the vote counted. One of ordinary skill in the art would have been motivated to perform such a modification because of the use of the Internet presents an opportunity to make voting more convenient (see '793 col. 1 lines 43 et seq.) "The rising importance of the internet and other forms of electronic communication in the United States of America and abroad presents a unique opportunity to reduce the inconvenience and expense associated with traditional voting systems. However, there are a considerable number of concerns about security and privacy which will

have to be met before the internet and/or other forms of electronic communication becomes viable as a substitute for or supplement to traditional paper ballot type elections”.

As to dependent claim 4, “wherein the combined confirmation message is obtained using concatenating content from each of the first and second confirmation messages” is taught in ‘793 col. 10, lines 6-33.

As to dependent claim 19, “further comprising: receiving a ballot choice confirmation message corresponding to a ballot choice received for the voter at a ballot collection entity; and displaying the received ballot choice confirmation message so that the recipient can compare the displayed ballot choice confirmation message with the ballot choice confirmation message identified in the confirmation dictionary as corresponding to the ballot choice selected by the voter” is shown in ‘793 col. 10, lines 6-33.

As to independent claim 21, this claim contains substantially similar subject matter as claim 19; therefore it is rejected along similar rationale.

14. **Claims 6 and 7**, are rejected under 35 U.S.C. 103(a) as being unpatentable over ‘447 in further view of Kilian et al. U.S. Patent No. 5,682,430 (hereinafter ‘430).

As to dependent claim 6, the following is not taught in ‘447: “wherein each of the first and second confirmation messages contains a value, and wherein the combined confirmation message is obtained by determining the product of the values contained in the first and second confirmation values” however ‘430 teaches “A three-step procedure is followed by each mixing center ... The third step is proving that the centers correctly executed the first and second steps. The Fiat-Shamir technique as discussed in an article entitled "How to

Prove Yourself: Practical Solutions to identification and signature problems" in Advances in Cryptology--Crypto '86, Springer-Verlag, 1986, pp. 186 to 199, can be used to make the above proofs non-interactive ... Also, the invention results in a method which reduces the amount of communication and computation necessary to generate, transmit and check the proofs by combining multiple proofs into a single proof" in col. 2, lines 8-29.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '447 an electronic voting method to include a means where the confirmation contains determination of the product of values in the first and second messages. One of ordinary skill in the art would have been motivated to perform such a modification to verify the accuracy of votes cast (see '430 col. 1 lines 10 et seq.) "Secure electronic voting is one of the most important applications of secure multiparty computation. Yet despite extensive work on this subject, no complete solution has been found in either the theoretical or practical domains. Even the general solutions to secure multi-party protocols fail to exhibit all of the desired security properties of elections".

As to dependent claim 7, "wherein each of the first and second confirmation messages contains a first value and a second value, wherein the combined confirmation message is obtained by: determining the product of the first values contained in the first and second confirmation messages; and determining the product of the second values contained in the first and second confirmation messages" is taught in '430 col. 2, lines 8-29.

15. **Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over '447 in further view of Ono et al. U.S. Patent No. 6,523,115 (hereinafter '115).**

As to dependent claim 8 the following is not taught in '447: **“further comprising receiving a third confirmation message from a third party that is independent of the first and second parties, the content of the third confirmation message independently confirming the identity of the ballot choice received for the voter by the vote collection authority”** however '115 teaches “The above object may be also achieved by the device decrypting a ciphertext outputted from an encryption device, ... a first generating unit for generating third verification data by performing an algorithm corresponding to the first message digest algorithm for the decrypted plaintext; a first verification unit for verifying the received first verification data using the third verification data; a second generating unit for generating fourth verification data by performing an algorithm corresponding to the second message digest algorithm for a combination of the received first verification data and the received ciphertext; a second verification unit for verifying the received second verification data using the fourth verification data; and an outputting unit for outputting results of the first verification unit and the second verification unit” in col. 5, lines 45-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '447 an electronic voting method to include a means where the transmitted data can be confirmed using multiple encryption schemes. One of ordinary skill in the art would have been motivated to perform such a modification to account for the difficulties when transmitting encrypted data (see '115 col. 1 lines 10 et seq.) “In the above e-mail encryption system, a message addressed to a plurality of recipients is encrypted once to generate a single ciphertext that is broadcast to the recipients. However, should mail recipient 1505 mistakenly use secret key 1524, instead of secret key 1523, to decrypt a message that has been

Art Unit: 2134

encrypted with public key 1521, the encrypted message will not be correctly decrypted. In other cases, errors during transmission can result in a partial loss of the ciphertext or in mistransmission of its content. Here also, the encrypted message will not be correctly decrypted. In this way, a mail recipient having two or more secret keys can't know, whether a failure to correctly decrypt a ciphertext is due to the use of the wrong secret key or an error during transmission".

16. **Claims 19** is rejected under 35 U.S.C. 103(a) as being unpatentable over '447 in further view of Pykälistö U.S. Patent No. 5,970,385 (hereinafter '385).

As to dependent claim **23**, the following is not taught in '447: "**wherein the second transmission system sends the confirmation dictionary guide via a voice message**" however '385 teaches "The instructions concern the processing of a call participating in a televote and they contain, for example, instructions about the announcement that will be given to a network user participating in a televote. In accordance with the IN standards, the voters are given a single, always similar, voice message. An example for such a message is: 'You have phoned to a televote on the Eurovision Song Contest. Your vote has been registered. Thank you for calling'" in col. 3, lines 56-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of '447 an electronic voting method to include a means where confirmation information is distributed by voice. One of ordinary skill in the art would have been motivated to perform such a modification in order to use different available communication methods to verify vote (see '447 col. 7 lines 40-48) "via an arbitrary communication channel ...

The access to the authorized-voter list 240B can be made, for example, using a predetermined telephone number”.


Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 2:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
3 November 2005


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100